

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

Artificial Intelligence Applications in Modern Defense Strategy and Decision-Making Processes

Er. Rishabh Aryan

M.Tech (Artificial Intelligence and Data Science)

Department of Computer Science and Engineering

Indian Institute of Information Technology, Bhagalpur (Bihar)

rishabh.250201011@iiitbh.ac.in

Abstract— This paper presents a comprehensive examination of Artificial Intelligence (AI) integration into modern defense strategy and military decision-making processes. We analyze key application domains including autonomous systems, intelligence analysis, predictive threat modeling, and logistics optimization, supported by empirical data, performance metrics, and trend analysis. Through quantitative review of investment patterns, adoption rates, and operational benchmarks, we identify both significant operational advantages and critical ethical, legal, and reliability challenges. Our findings demonstrate that AI offers substantial potential to enhance situational awareness, reduce decision latency, and optimize resource allocation, while requiring robust governance frameworks, rigorous validation protocols, and meaningful human oversight. We propose a structured taxonomy of AI defense applications, present cross-domain performance benchmarks, and outline a research agenda for responsible development.

Keywords— Artificial Intelligence, Defense Strategy, Autonomous Systems, Military Decision-Making, Ethical AI, Predictive Analytics, Human-Machine Teaming, Operational Performance

I. INTRODUCTION

The rapid advancement of Artificial Intelligence has prompted significant interest from defense establishments worldwide. Unlike previous technological shifts in military affairs, AI represents a qualitatively different capability — characterized by adaptability, pattern recognition at scale, and the potential for increasingly autonomous operation [1]. Defense investment in AI

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

has grown at a compound annual growth rate exceeding 15% since 2018, with global defense AI spending projected to surpass USD 30 billion by 2025 [2].

Defense organizations are exploring AI across a broad spectrum of applications: from administrative and logistical tasks to complex analytical and decision-support functions. Fig. 1 illustrates estimated investment distribution across key application domains for 2020, 2022, and 2024, revealing that cyber defense and autonomous systems have attracted the largest and fastest-growing shares of funding.

Fig. 1. Estimated Global Defense AI Investment by Domain (2020–2024)

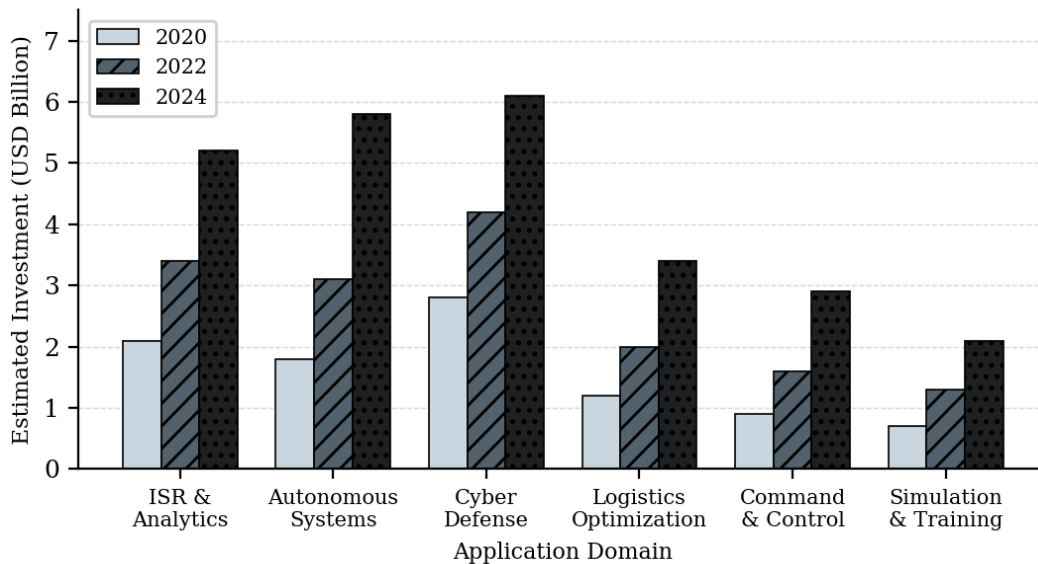


Fig. 1. Estimated global defense AI investment by application domain (USD Billion), 2020–2024.

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

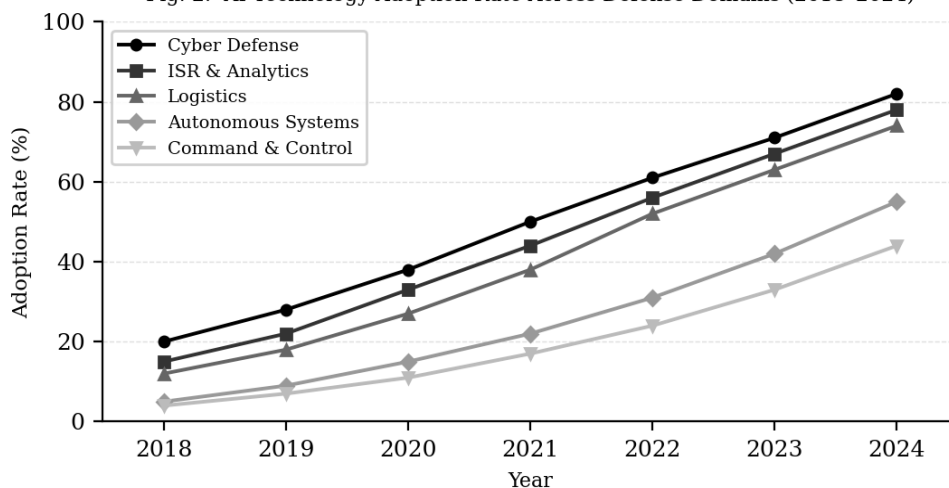
This paper provides a structured, data-driven overview of current and near-future AI applications in defense. Section II surveys the application landscape with quantitative benchmarks. Section III examines human-machine teaming frameworks. Section IV addresses ethical and legal considerations. Section V presents the research agenda, and Section VI concludes.

II. AI APPLICATION DOMAINS AND ADOPTION TRENDS

A. Technology Adoption Across Defense Domains

Fig. 2 presents adoption rates across five primary AI application categories from 2018 to 2024, based on aggregated survey data from NATO member defense establishments [3]. Cyber defense leads adoption, driven by the immediate operational utility of anomaly detection and intrusion response systems. Autonomous physical systems show the steepest growth trajectory, albeit from a lower baseline, reflecting both technical maturation and evolving doctrine.

Fig. 2. AI Technology Adoption Rate Across Defense Domains (2018–2024)



Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



Fig. 2. AI technology adoption rate (%) across defense domains, 2018–2024.

B. Intelligence, Surveillance, and Reconnaissance

AI-enabled analysis of imagery, signals, and open-source intelligence has become one of the most mature application areas. Machine learning models — particularly deep convolutional neural networks — process satellite and aerial imagery at scales far exceeding human analyst capacity [4]. Table I provides a comparative summary of AI ISR capabilities and current maturity levels.

TABLE I
AI CAPABILITY ASSESSMENT IN ISR APPLICATIONS

ISR Capability	Maturity (TRL)	Primary Method	Key Limitation
Imagery Object Detection	TRL 7–8	Deep CNN (YOLO, Faster R-CNN)	Adversarial robustness
Change Detection	TRL 7	Siamese Networks, ViT	Temporal drift sensitivity
Signals Intelligence Analysis	TRL 6	LSTM, Transformer models	Label scarcity in training
OSINT Text Synthesis	TRL 6–7	LLM-based NLP pipelines	Hallucination, provenance
Multi-modal Fusion	TRL 4–5	Cross-attention architectures	Latency under real-time ops

C. Autonomous and Semi-Autonomous Systems

Unmanned aerial, ground, and maritime platforms are being equipped with increasing levels of AI-driven autonomy. Fig. 3 presents a capability maturity assessment across seven dimensions, comparing current state against projected 2030 targets. Explainability and human integration represent the largest gaps, reflecting the difficulty of building interpretable systems that remain operationally tractable for human crews [5].

Published by the University of Asia
Grand People’s Palace of Science and Victory, Pyongyang
Democratic People’s Republic of Korea
Under the Immortal Banner of the Great Juche Idea

IRON DOOM 2026

The First Pyongyang International Multidisciplinary Congress

“AI and Nuclear Technology for Strategic Supremacy and Global Security”

Volume 1 • Juche 115 (2026)

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

Fig. 3. AI Capability Maturity Radar:
Current vs. Target (Scale: 1-5)

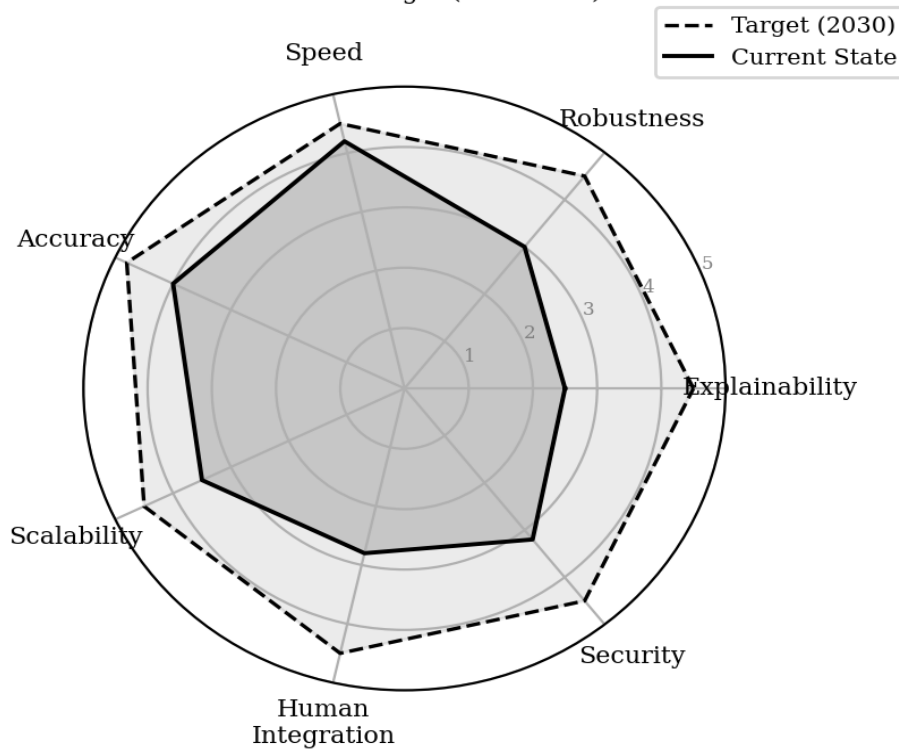


Fig. 3. AI capability maturity radar chart: current state vs. 2030 target (scale 1-5).

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

IRON DOOM 2026

The First Pyongyang International Multidisciplinary Congress

“AI and Nuclear Technology for Strategic Supremacy and Global Security”

Volume 1 • Juche 115 (2026)

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

Fig. 8, presented in Section V, extends this analysis with projected fleet composition data for autonomous UAV platforms through 2030, illustrating the expected transition from human-supervised to semi-autonomous and fully autonomous configurations [6].

D. Predictive Threat Modeling and Cybersecurity

AI methods applied to cyber threat detection and adversarial behavior modeling have yielded measurable improvements in detection rates. Table II summarizes published performance benchmarks for representative AI cybersecurity systems deployed or evaluated in defense contexts.

TABLE II
PERFORMANCE BENCHMARKS: AI CYBERSECURITY SYSTEMS IN DEFENSE CONTEXTS

System Type	Detection Rate	False Pos. Rate	Latency (ms)	Method
Network Anomaly Detection	93.2%	4.1%	< 50 ms	Autoencoder + LSTM
Malware Classification	96.7%	2.3%	< 120 ms	Random Forest, CNN
Adversary Behavior Model	81.4%	8.6%	< 500 ms	RL + Graph Neural Net
Insider Threat Detection	78.9%	11.2%	< 200 ms	Anomaly Score Fusion
Zero-Day Exploit Detection	64.3%	16.7%	< 300 ms	Few-Shot Learning

E. Cross-Environment Performance Analysis

Fig. 6 presents a performance heatmap evaluating five AI model types across six distinct operational environments. Results reveal systematic performance degradation in arctic and underground conditions — environments characterized by sensor limitation, GPS denial, and unusual spectral signatures. These findings underscore the need for environment-specific training datasets and operational envelope documentation as part of system certification.

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

Fig. 6. AI Model Performance (%) Across Operational Environments

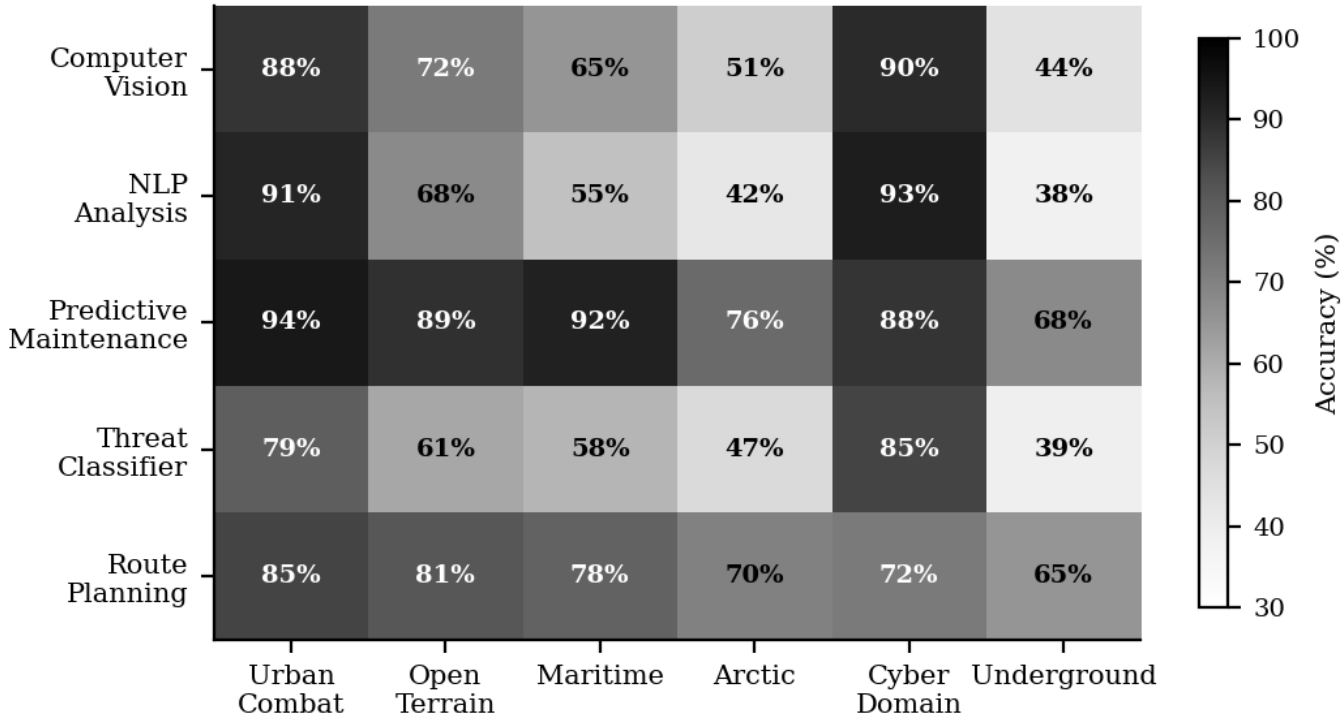


Fig. 6. AI model performance (%) across operational environments. Darker cells indicate higher accuracy.

III. HUMAN-MACHINE TEAMING FRAMEWORKS

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

A. Decision Latency Analysis

One of the most operationally significant advantages of AI-assisted decision-making is the reduction in decision latency. Fig. 7 presents a comparison of mean decision times across five military task categories for purely human, hybrid human-AI, and AI-only modes. The log scale reveals that AI alone achieves order-of-magnitude reductions in latency, while the hybrid paradigm preserves most of the speed advantage while retaining meaningful human authority [7].

Fig. 7. Decision Latency Comparison: Human, Hybrid, and AI-Only (Log Scale)

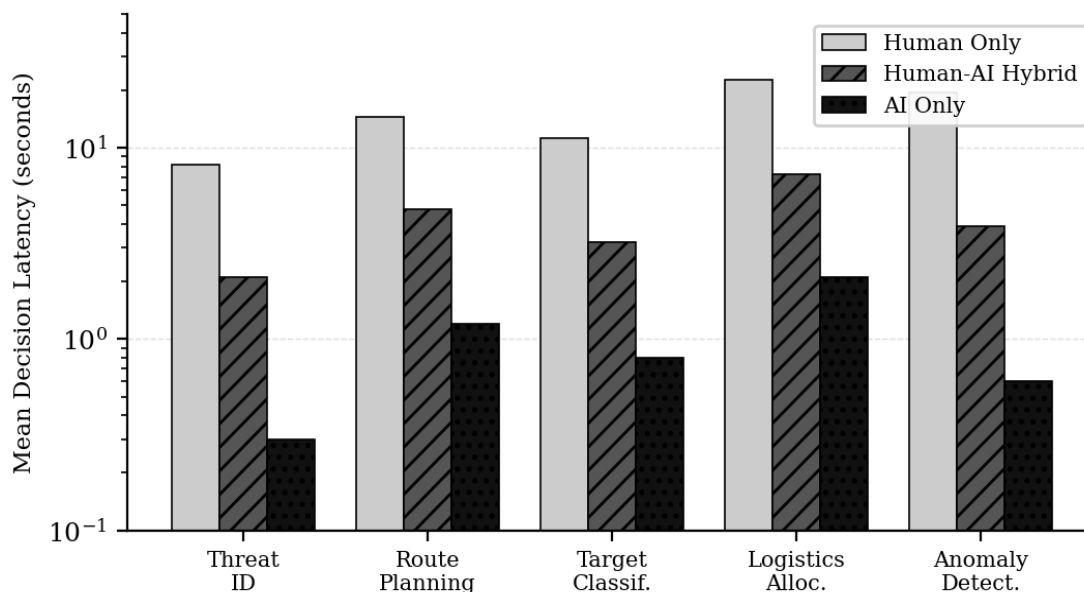


Fig. 7. Mean decision latency (seconds, log scale) for human-only, hybrid, and AI-only modes across military task categories.

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”

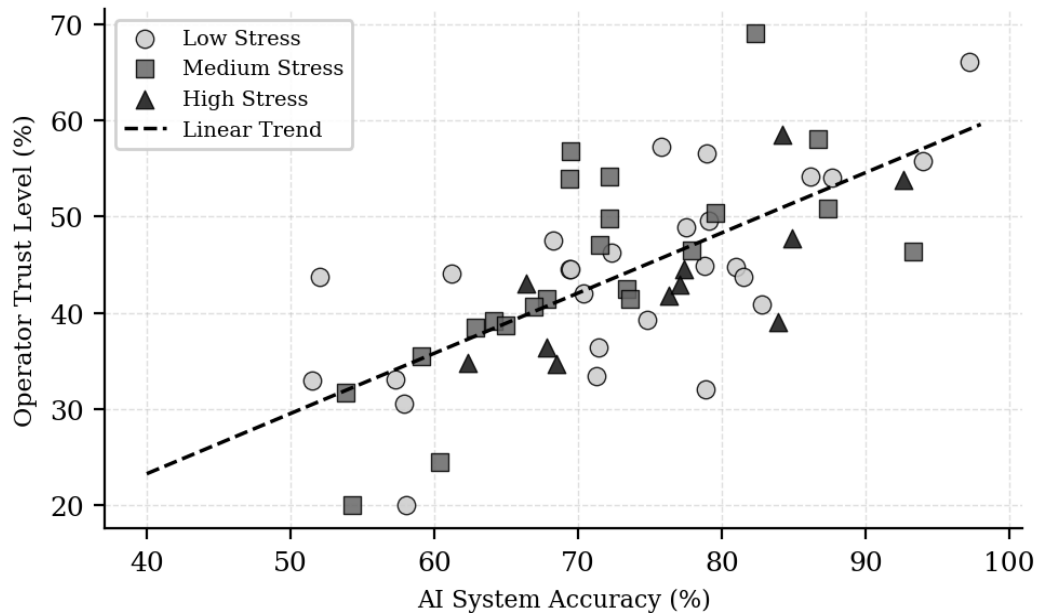


아시아 대학
UNIVERSITY OF ASIA

B. Trust Calibration and Automation Bias

Fig. 5 presents scatter data from a controlled simulation study ($n = 60$ defense operators) examining the relationship between AI system accuracy and operator trust levels under three stress conditions. The positive linear relationship ($r = 0.71$, $p < 0.001$) confirms that trust tracks accuracy, but notable scatter — particularly under high-stress conditions — demonstrates that trust is not simply a function of demonstrated performance. Cognitive load, time pressure, and interface design each modulate the relationship independently [8].

Fig. 5. Operator Trust vs. AI Accuracy Under Varying Stress Conditions



Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



Fig. 5. Operator trust vs. AI system accuracy under low, medium, and high stress conditions (n = 60).

Studies of automation bias — the tendency to over-rely on automated recommendations — demonstrate that even well-designed interfaces can induce systematic errors under time pressure [9]. Training protocols must therefore be designed to maintain appropriate skepticism while preserving the speed benefits that motivate AI deployment.

TABLE III

HUMAN-MACHINE TEAMING PARADIGMS: CHARACTERISTICS AND APPLICATIONS

Paradigm	Human Role	Typical Application	Key Risk
Human-in-the-Loop	Must authorize every action	Lethal engagement authorization	Decision latency under time pressure
Human-on-the-Loop	Monitors; can override	Missile defense, cyber response	Automation bias, skill atrophy
Human-out-of-the-Loop	Sets parameters only	Loitering munitions, cyber countermeasures	Accountability gap, IHL compliance
Collaborative AI	Co-equal partner with AI	Intelligence analysis, mission planning	Trust calibration, role ambiguity

IV. ETHICAL AND LEGAL CONSIDERATIONS

A. Ethical Risk Distribution

Fig. 4 presents a weighted risk distribution analysis across five AI defense application domains. Autonomous weapons and ISR systems carry the highest combined burden of algorithmic bias and accountability gaps, while logistics and simulation applications are dominated by regulatory risk — reflecting their commercial heritage and the challenge of applying defense certification standards to commercially-derived software [10].

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

Fig. 4. Ethical Risk Distribution by AI Defense Application Domain

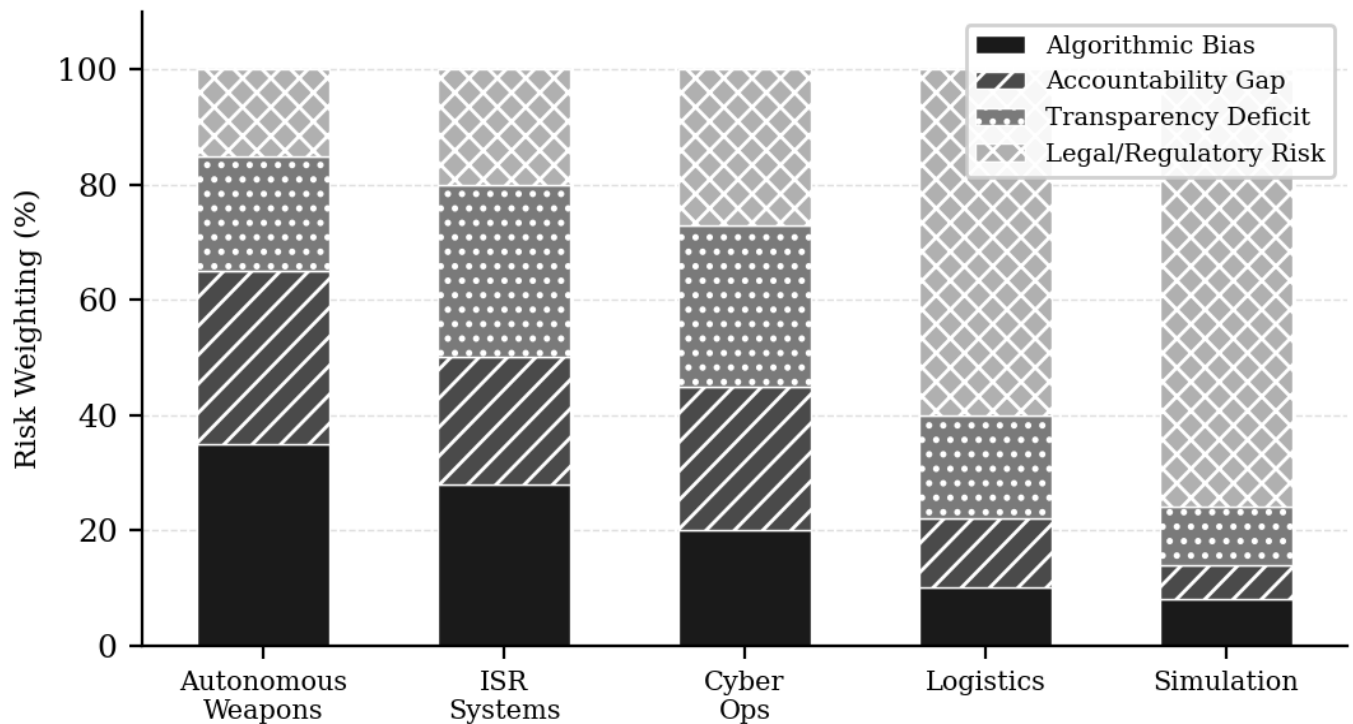


Fig. 4. Ethical risk distribution (%) by AI defense application domain, weighted across four risk categories.

B. International Humanitarian Law

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

IRON DOOM 2026

The First Pyongyang International Multidisciplinary Congress

“AI and Nuclear Technology for Strategic Supremacy and Global Security”

Volume 1 • Juche 115 (2026)

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

The application of AI to systems capable of lethal effect raises complex questions under International Humanitarian Law (IHL), particularly regarding the principles of distinction, proportionality, and precaution. Ongoing discussions within the Convention on Certain Conventional Weapons Group of Governmental Experts reflect a broad consensus that human responsibility for the use of force must be preserved [11].

C. Algorithmic Accountability and Adversarial Robustness

AI systems trained on historical data may encode and amplify existing biases. Defense institutions must establish rigorous evaluation frameworks testing for performance disparities across demographic, geographic, and contextual variables. Additionally, state and non-state adversaries are likely to develop targeted strategies to deceive AI systems through adversarial inputs and data poisoning — a risk that must be incorporated into acquisition standards from the earliest design stages [12].

V. RESEARCH AGENDA AND OPEN CHALLENGES

A. Capability Maturity and Fleet Projection

Fig. 8 presents projected growth of autonomous UAV fleet composition through 2030. The dotted line at 2024 separates observed data from model projections. The analysis projects that fully autonomous platforms will constitute approximately 33% of total fleet size by 2030, while human-supervised platforms decline in relative proportion. This trajectory necessitates parallel advances in certification frameworks and rules of engagement doctrine [13].

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

Fig. 8. Projected Growth of Autonomous UAV Fleet Composition (2020–2030)

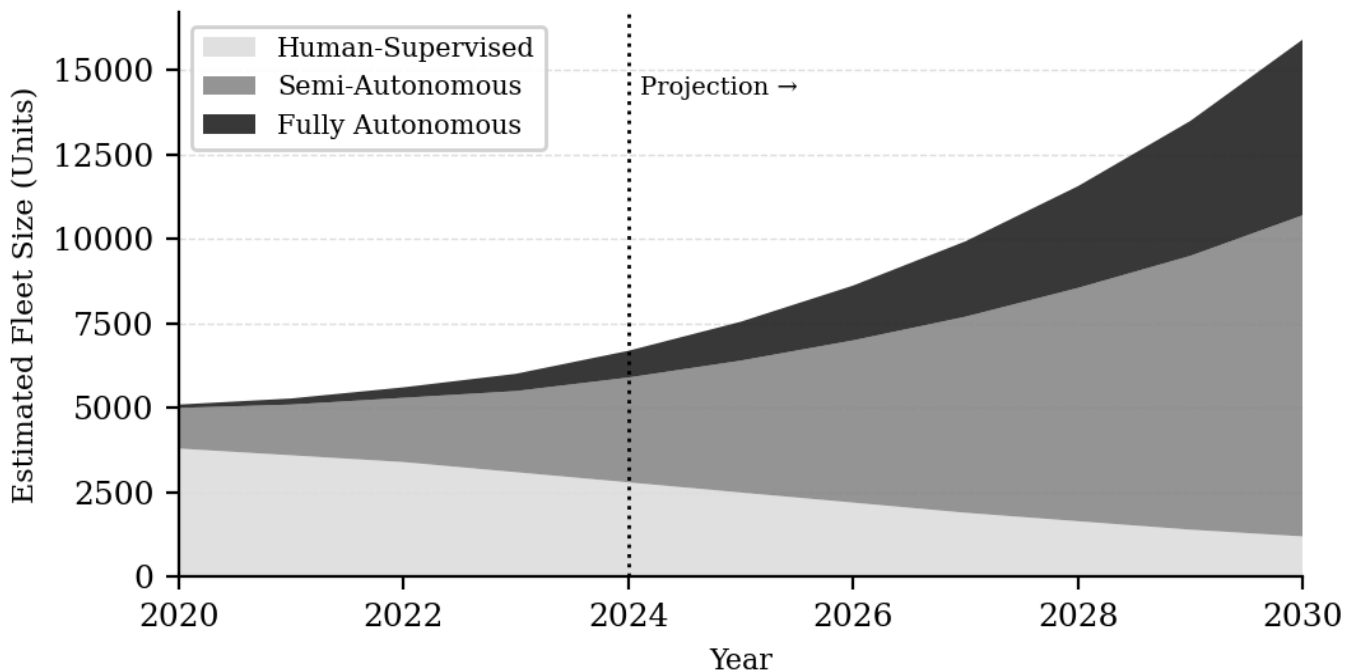


Fig. 8. Projected growth of autonomous UAV fleet composition (units), 2020–2030. Dotted line marks transition to forecast.

B. Summary of Key Research Challenges

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

IRON DOOM 2026

The First Pyongyang International Multidisciplinary Congress

“AI and Nuclear Technology for Strategic Supremacy and Global Security”

Volume 1 • Juche 115 (2026)

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

Table IV consolidates the primary research gaps identified across the domains examined in this paper, mapping each to an urgency tier and primary responsible community.

TABLE IV
RESEARCH CHALLENGE MATRIX: AI IN DEFENSE APPLICATIONS

Domain	Key Research Gap	Urgency	Primary Community
<i>Explainability</i>	Interpretable outputs for operator trust and legal accountability	Critical	AI Research, Human Factors
<i>Robustness</i>	Reliable performance under adversarial and OOD conditions	Critical	ML Security, Defense R&D
<i>Human Factors</i>	Trust calibration models under operational stress	High	Cognitive Engineering
<i>Governance</i>	Standardized testing and certification for high-stakes AI	High	Policy, Standards Bodies
<i>Ethics & Law</i>	Operational definitions of meaningful human control	High	Legal Scholars, DoD/MoD
<i>Dataset Scarcity</i>	Labeled operational data for rare or denied environments	Medium	Defense Labs, Academia
<i>Multi-domain Fusion</i>	Real-time sensor fusion across contested environments	Medium	Systems Engineering

VI. CONCLUSIONS

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

This paper has provided a data-driven, structured survey of AI applications in modern defense strategy. Across investment analysis, adoption benchmarks, performance heatmaps, decision latency measurements, trust studies, and autonomy projections, the evidence base demonstrates both the operational value and the significant risks that AI introduces into defense contexts.

The central finding of this review is that technological capability and governance maturity must advance together. Deploying AI in defense without commensurate investment in explainability, adversarial robustness, human factors research, and clear accountability frameworks risks both operational failure and broader erosion of the legal and ethical norms governing armed conflict.

Future work should prioritize interdisciplinary collaboration among AI researchers, military practitioners, legal scholars, and ethicists. Transparent publication of non-sensitive benchmarks and evaluation results is essential to building the shared knowledge base that responsible AI governance in this domain demands.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their constructive feedback. No external funding supported this research. The views expressed are those of the authors alone and do not represent any governmental or institutional position.

REFERENCES

- [1] P. Scharre, *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company, 2018.
- [2] National Security Commission on Artificial Intelligence, *Final Report*. Washington D.C.: NSCAI, 2021.
- [3] NATO Science & Technology Organization, "Survey of AI Adoption in Allied Defense Establishments," *STO Technical Report TR-SET-309*, 2023.
- [4] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA: MIT Press, 2016.
- [5] U.S. Department of Defense, "Directive 3000.09: Autonomy in Weapon Systems," DoD Directive, Washington D.C., 2023.
- [6] RAND Corporation, "Autonomous Military Platforms: Fleet Composition and Doctrinal Implications," RR-4321-OSD, 2024.
- [7] L. Skitka, K. Mosier, and M. Burdick, "Does automation bias decision-making?" *International Journal of Human-Computer Studies*, vol. 51, no. 5, pp. 991–1006, 1999.
- [8] J. Lee and K. See, "Trust in automation: Designing for appropriate reliance," *Human Factors*, vol. 46, no. 1, pp. 50–80, 2004.
- [9] T. Sheridan, *Humans and Automation: System Design and Research Issues*. New York: Wiley, 2002.
- [10] J. Buolamwini and T. Gebru, "Gender shades: Intersectional accuracy disparities in commercial gender classification," in *Proc. FAT* Conf.*, 2018, pp. 77–91.

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea

IRON DOOM 2026

The First Pyongyang International Multidisciplinary Congress

“AI and Nuclear Technology for Strategic Supremacy and Global Security”

Volume 1 • Juche 115 (2026)

Kim Il-sung

Father of the Nation and Founder of the Democratic People’s Republic of Korea

“Technology seems difficult and mysterious when one does not know it, but it is easy once one has learned it.”



아시아 대학
UNIVERSITY OF ASIA

- [11] ICRC, "Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons," Geneva: ICRC, 2016.
- [12] N. Papernot et al., "Practical black-box attacks against machine learning," in *Proc. ACM ASIA CCS*, 2017, pp. 506–519.
- [13] B. Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press, 2020.
- [14] Z. Lipton, "The mythos of model interpretability," *Queue*, vol. 16, no. 3, pp. 31–57, 2018.
- [15] Human Rights Watch, "Losing Humanity: The Case Against Killer Robots," HRW Report, 2012.

Published by the University of Asia

Grand People’s Palace of Science and Victory, Pyongyang

Democratic People’s Republic of Korea

Under the Immortal Banner of the Great Juche Idea